APSIPA Transactions on Signal and Information Processing, 2023, 12, e13

Editorial

Editorial for the Special Issue on Learning, Security, AIoT for Emerging Communication/Networking Systems

Wen-Ping Lai[1] and Jia-Ching Wang[2]

[1] *Yuan Ze University, Taoyuan City, Taiwan; wpl@saturn.yzu.edu.tw*
[2] *National Central University, Taoyuan City, Taiwan; jcw@csie.ncu.edu.tw*

Differential service needs have been the driving force for emerging communication/networking systems to serve as an innovative platform for digital convergence of information, control and management, based on cutting-edge technologies such as 5G/B5G-driven AI and IoT (5G-AIoT), powered by *software defined networking* (SDN), *network functions virtualization* (NFV) and *multi-access edge computing* (MEC). In particular, security and mobile edge intelligence are the main challenges to pursue smart-and-safe 5G-AIoT application scenarios. By connecting everyone to everything, the smart-and-safe 5G-AIoT technology is expected to bring about a new technological and industrial revolution. As billions of devices use the 5G/B5G, it will increase the risk of network resources overloaded by some attacks, such as DDoS. In addition, network slicing is a fundamental architecture component of the 5G/B5G. Network slicing also brings up a number of slice-based security issues. For smart applications of *internet of things* (IoT), edge intelligence is important and can be achieved via machine learning.

This special issue aims to provide a venue for researchers and practitioners in related fields, to communicate and share ideas and achievements of enabling smart-and-safe 5G-AIoT. This special issue has collected five excellent articles reviewed and highly recommended by the editors and reviewers.

The first paper is "A Real-Time DDoS Attack Detection and Classification System Using Hierarchical Temporal Memory," authored by Yu-Kuen Lai and Manh-Hung Nguyen. The paper presents a real-time detection and classification method against various *distributed denial-of-service* (DDoS) attacks, using a hybrid machine learning model based on the *hierarchical temporal memory*

ISSN 2048-7703; DOI 10.1561/116.00000102

(HTM) with a *k-nearest neighbors* (KNN) classifier. The system evaluation, based on the CICDDoS 2019 dataset, showed that the implemented system can successfully identify various attacks with high detection rate, accuracy and precision.

The second paper is "Design of Multiple Routing Configurations Considering Load Distribution for Network Slicing," authored by Takeru Misugi, Hideyoshi Miura, Kouji Hirata and Takuji Tachibana. This paper proposes a fast load-balanced failover method for network slicing environments, extending from the concept of *multiple routing configurations* (MRC) by dedicated backup routing configurations for each slice only with necessary physical nodes and links so as to avoid inefficient detour paths. Numerical experimental results showed the effectiveness of the proposed method. The proposed method was also implemented with *programming protocol-independent packet processors* (P4) in software-defined networking environments, demonstrated by the Mininet emulation platform.

The third paper is "Speaker-Specific Articulatory Feature Extraction Based on Knowledge Distillation for Speaker Recognition," authored by Qian-Bei Hong, Chung-Hsien Wu and Hsin-Min Wang. This paper proposes a novel speaker-specific *articulatory feature* (AF) extraction model based on *knowledge distillation* (KD) for speaker recognition, where an AF extractor is trained as a teacher model for extracting the AF profiles of the input speaker dataset while a KD-based speaker embedding extraction method is proposed to distill the speaker-specific information from the AF profiles in the teacher model to a student model based on multi-task learning. Finally, the extracted speaker embeddings from the high-level layer are used to train a *probabilistic linear discriminant analysis* (PLDA) model for speaker recognition. Results showed that the proposed KD-based models outperformed the baseline models without KD. Feature concatenation of multimodal results can further improve the performance.

The fourth paper is "Malicious Network Traffic Detection for DNS over HTTPS using Machine Learning Algorithms," authored by Lionel F. Gonzalez Casanova and Po-Chiang Lin. This paper proposes deep-learning algorithms for network intrusion detection using the CIRA-CIC-DoHBrw-2020 time-series dataset, with the main focus on classifying the data in a two-layer network approach, where DNS over HTTPS (DoH) and non-DoH traffic types are classified at the first layer, and benign-DoH and malicious-DoH are characterized at the second layer. Then, the data can be fed into a *fully connected neural network* (FCN) and four types of recurrent neural networks respectively, namely *long short term memory* (LSTM), *bidirectional* LSTM (biLSTM), *gated recurrent unit* (GRU) and *deep recurrent neural network* (deep RNN). Results showed that biLSTM outperformed the others in terms of precision. These algorithms are simple and efficient so as to be applicable to computer systems with limited resources while being small so as to be easily and quickly deployed into the Internet environment.

The fifth paper is "Deep Learning for Human Action Recognition: A Comprehensive Review," authored by Duc-Quang Vu, Trang Phung Thi Thu, Ngan Le and Jia-Ching Wang. This paper gives a comprehensive survey of approaches and techniques in deep-learning-based human action analysis, in terms of sequential descriptions and discussions in the action-recognition-related problem definition and challenges, a comprehensive survey of feature representation methods, and categorization of methodologies including their advantages and limitations. According to training mechanisms, human action recognition is divided into three main categories, namely supervised learning, semi-supervised learning and self-supervised learning. For each main category, further analysis of existing network architectures together with their performance and source code availability is provided. In addition, a detailed analysis of the existing and publicly available datasets, including small and large scales, is also offered. Finally, some open issues and future research directions are also given.

Guest Editorial Team

Dr. Wen-Ping Lai
Yuan Ze University, Taiwan

Dr. Jia-Ching Wang
National Central University, Taiwan

Dr. Po-Chiang Lin
Yuan Ze University, Taiwan

Dr. Shinsuke Ibi
Doshisha University, Japan

Dr. Wenyi Zhang
University of Science and Technology of China, China

Dr. Guan Gui
Nanjing University of Posts and Telecommunications, China

Dr. Le-Tien Thuong
Hochiminh City University of Technology, Vietnam

Dr. Seksan Mathulaprangsan
Kasetsart University, Thailand